RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: LAB1-W01

When Things Go Boom! Your Supply Chain Risk

Dr. Chris Pierson
CEO
BlackCloak
www.BlackCloak.io

James T. Shreve
Partner
Troutman Pepper Locke
www.troutman.com

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

- Introductions
- Setting the Stage – Overview of Supply Chain Risks
- Scenario
- Part I – Assessment, Risk Review, Mitigation Plan
- Part II – Boom!
- Application & Next Steps
- Questions

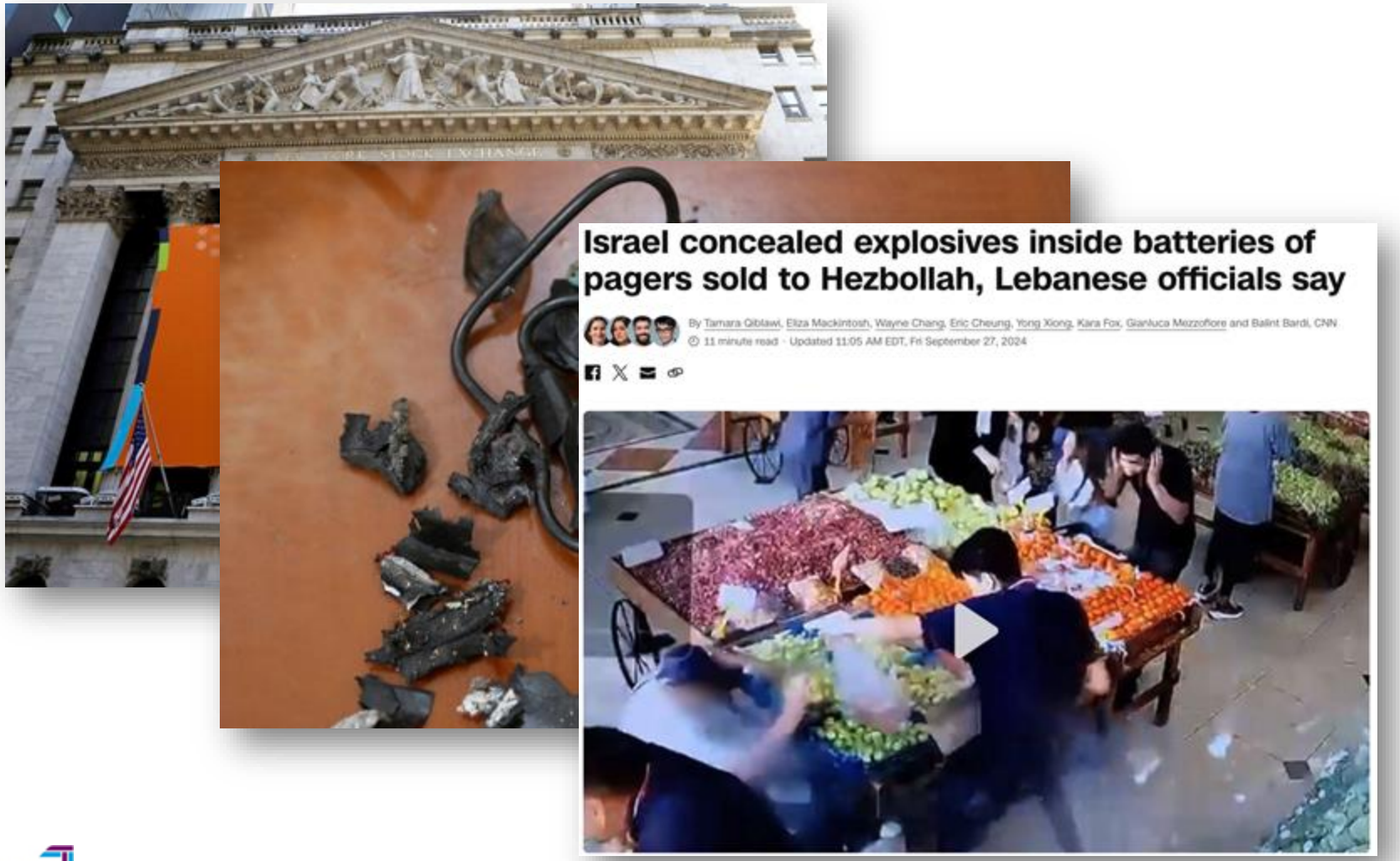
RSAC 2025 Conference

Setting The Stage

Getting Everyone Up to Speed

Types of Supply Chain Attacks

- Motivation
  - Economic
  - Ideological
  - Chaos/Vengeance
- Types
  - Software
  - Hardware


Israel concealed explosives inside batteries of pagers sold to Hezbollah, Lebanese officials say
By Tamara Qiblawi, Eliza Mackintosh, Wayne Chang, Eric Cheung, Yong Xiong, Kara Fox, Gianluca Mezzofiore and Balint Bardi, CNN
11 minute read · Updated 11:05 AM EDT, Fri September 27, 2024

Impacts of Supply Chain Attacks

- Targets
  - Company
  - Customer
  - 4th Party Cos.
- Impacts
  - Financial
  - Data
  - Reputation/Trust

Widely Used Software Company May Be Entry Point for Huge U.S. Hacking
Russian hackers may have piggybacked on a tool developed by JetBrains, which is based in the Czech Republic, to gain access to federal government and private sector systems in the United States.
Share full article
Officials are investigating whether a Russian company, based in the Czech Republic, was a pathway for Russian hackers to insert malware that would flow to a number of technology companies. Kirill Kudryavtsev/Agence France-Presse — Getty Images

RSAC 2025 Conference

Scenario

Our Company Today

Scenario

- Investment Firm
  - Seeking to analyze faster
  - Seeking to understand massive amounts of data
  - Outperform competitors
- Management Committee
  - Use AI to get ahead
  - Make advisors more empowered
  - Give advisors an alternative to individual research

Scenario - AI Project

- Seeking platform basis
- Will acquire and modify an interface for public AI platforms designed for use by investment firms
- Examine special AI Interface for
  - financial analysis
  - company research
  - market research
- Allow advisors to use online and offline searching
- StratGPT

RSAC 2025 Conference

Part I.

Risk Assessment, Review, Mitigation Plan

Risk Assessment, Review, Mitigation Plan

- Congratulations! You've been chosen to be part of the team reviewing the AI Project
- You understand this project is top of mind to Executive Management
- We know our competitors are working on a similar project
- Your task is to review the software, perform a risk assessment, and develop mitigation plans for any risks and present this to the Enterprise Risk Committee

Teams

- Security
- Legal
- Product/Engineering
- Privacy/Compliance
- Business Line

Time to Work

RSAC 2025 Conference

Part II.

Boom! - The Incident

Attack

- Your company has been using the interface for 6 months
- Cybercriminals know investment firms are using public AI platforms for many purposes
- Through an insider at the interface software company, a criminal group inserted malicious code into the interface
  - Code allows criminals to
    - Obtain prompts entered and results received by users
    - Modify the results to prompts to change information - e.g. dates, amounts, analysis

Attack

- The interface maker received reports from customers of suspicions about the interface in the last three months
- One month ago, the interface maker discovered the malicious code
- Yesterday, the interface maker alerted your company about the issue and provided a revised version of the interface
- Today's Wall Street Journal and Financial Times featured front page stories about the incident
- FINRA and the SEC reached out to the company to ask if the company had used the interface

Teams

- Security
- Legal/Privacy/Compliance
- Business Line
- Board & Senior Executives
- Public Relations/Marketing

Time to Work

RSAC 2025 Conference

What's Next?

How Do We Apply These Learnings?

Application – What's Next

- Next week you should:
  - Determine who owns "suppliers & vendors" in your company
- In the next three months you should:
  - Have meetings about risk registries/risks
  - Determine if adequate resources are being directed to this area
  - Ensure GRC around supplier risks
  - Determine top 10 vendors
- Within six months:
  - Develop a plan for addressing risks posed by Top 10
  - Ensure a GRC/Information Assurance Program is underway/funded
  - Determine whom at the Board & Exec level owns these programs
  - Conduct a Table Top Exercise around "supplier risk"
  - Set forth a schedule or plan to mitigate XX% of the highest risks your top vendors have
  - Ensure a robust plan is built for the next year

RSAC 2025 Conference

Many Voices.
One Community.

Thanks & Contact

Dr. Chris Pierson
BlackCloak
chris.pierson@blackcloak.io
www.blackcloak.io

James. T. Shreve
Troutman Pepper Locke
james.shreve@troutman.com
www.troutman.com